Figure 1

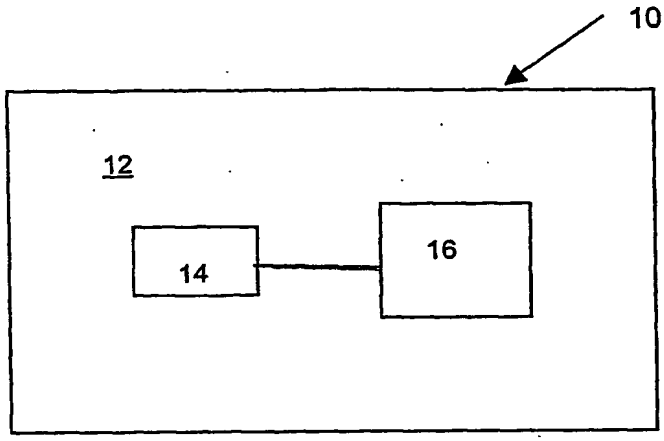
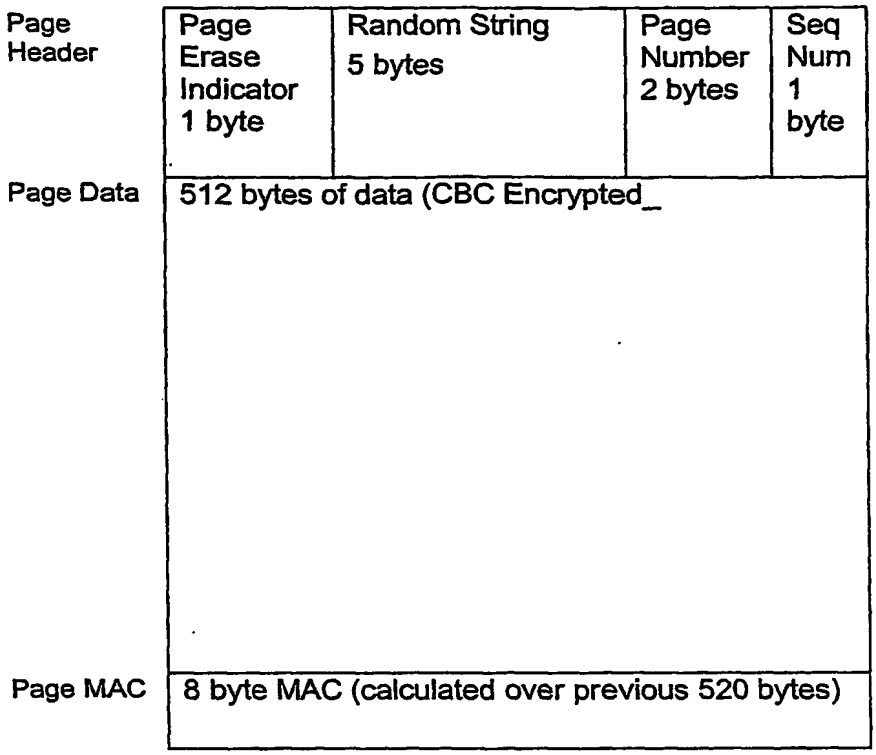


Figure 2


Page Header
Page Erase Indicator 1 byte
Random String 5 bytes
Page Number 2 bytes
Seq Num 1 byte
Page Data
512 bytes of data (CBC Encrypted_
Page MAC
8 byte MAC (calculated over previous 520 bytes)

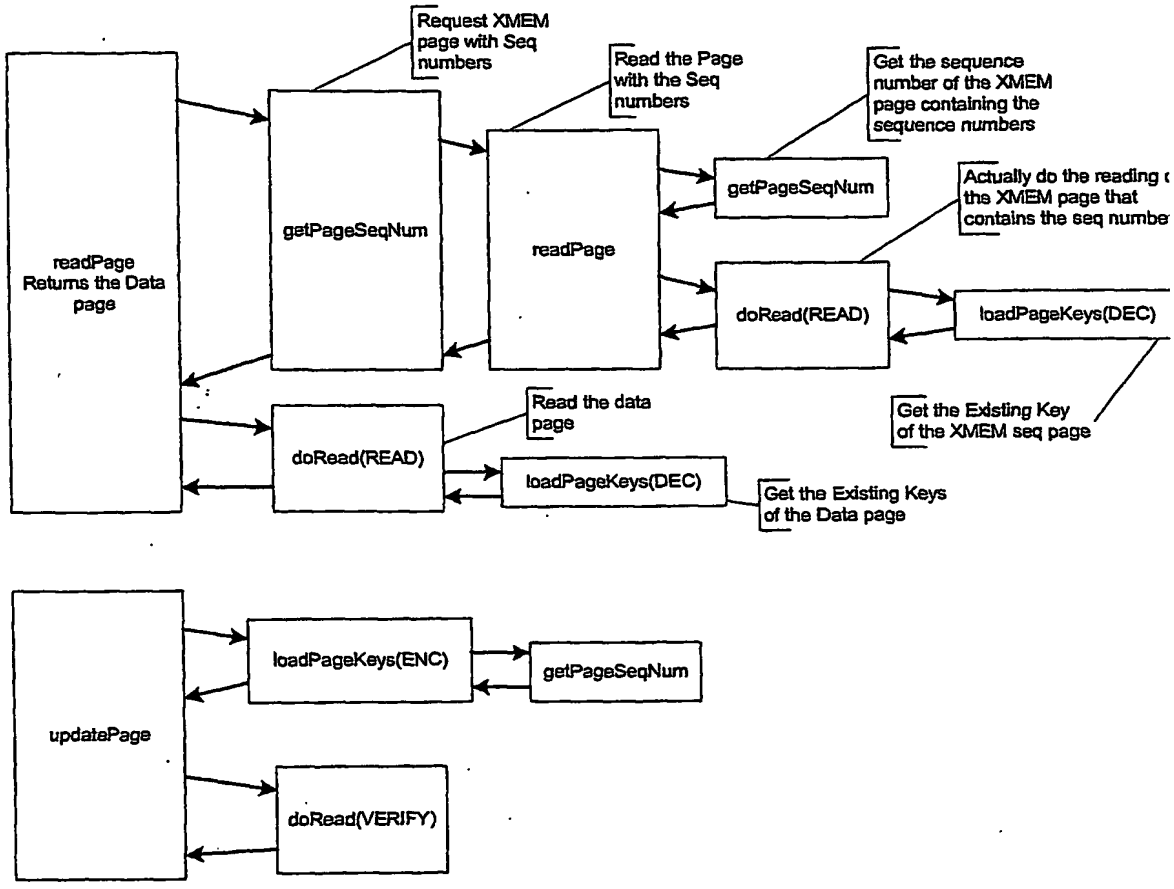

readPage
Returns the Data
page
getPageSeqNum
Request XMEM
page with Seq
numbers
readPage
Read the Page
with the Seq
numbers
getPageSeqNum
Get the sequence
number of the XMEM
page containing the
sequence numbers
doRead(READ)
Actually do the reading
the XMEM page that
contains the seq numbe
loadPageKeys(DEC)
Get the Existing Key
of the XMEM seq page
doRead(READ)
Read the data
page
loadPageKeys(DEC)
Get the Existing Keys
of the Data page
updatePage
loadPageKeys(ENC)
getPageSeqNum
doRead(VERIFY)

Figure 3